-= AVRFID =-

par tAd pour BlackLoop

Quoi ?

AVR (ATtiny85) + RFID = AVRFID

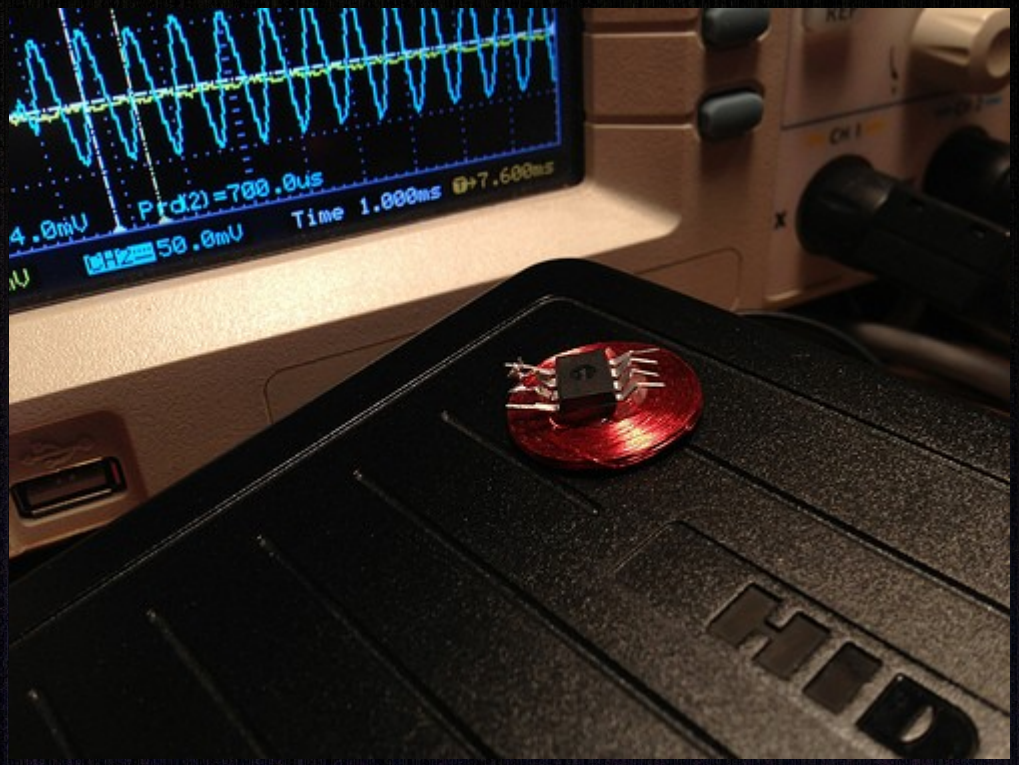
=> Emulation d'une carte RFID type
HID 'Proximity', 125 Khz (!= mifare!)

Qui ?

Projet de Micah 'Dowty' (Scanlime.org) documenté en septembre 2008.

Qui ?

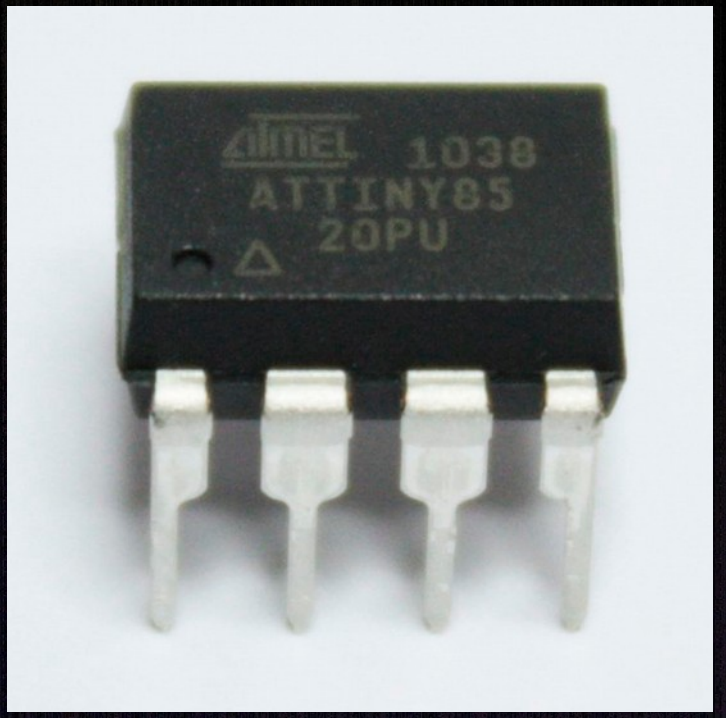
Code revu et optimisé, en C, par Trammell Hudson en 2012 puis 2013



Matériel ?

.Antenne faite main (bobine de cuivre, fin)

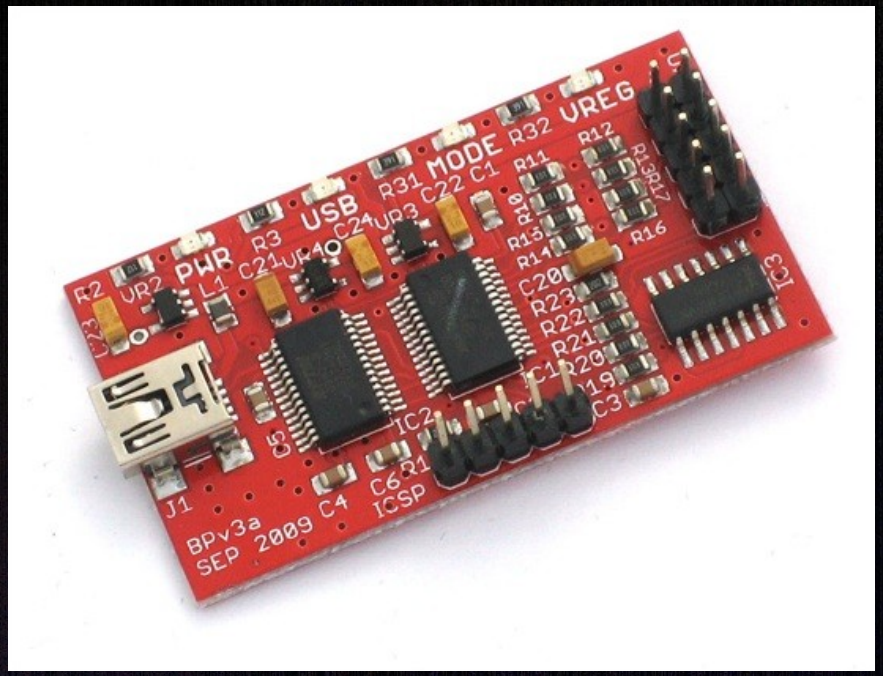
.ATtiny85 (+ de quoi le programmer)

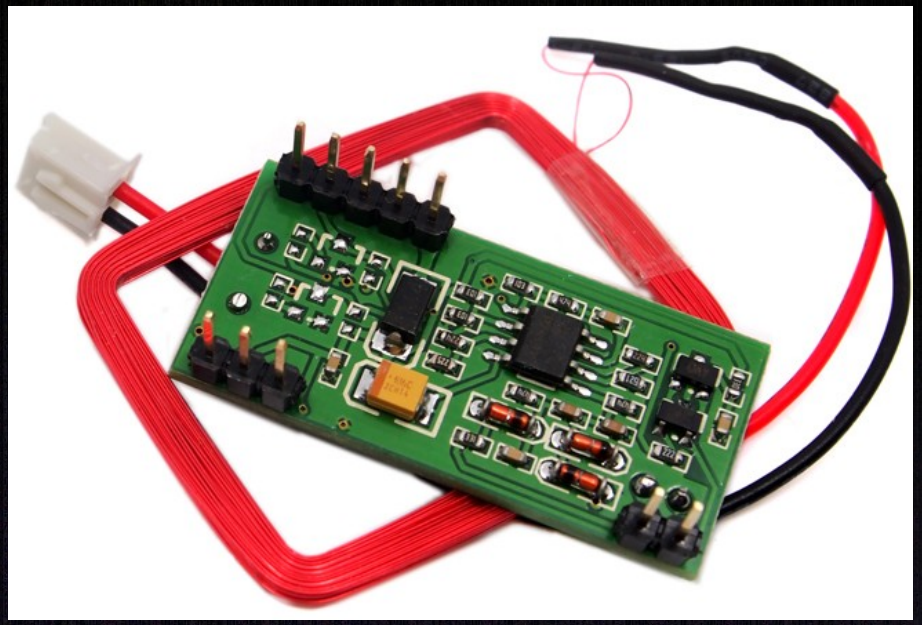


Matériel (suite) ?

.Bus Pirate pour programmation ATtiny

.Lecteur RFID 125 KHz (proxmark?)

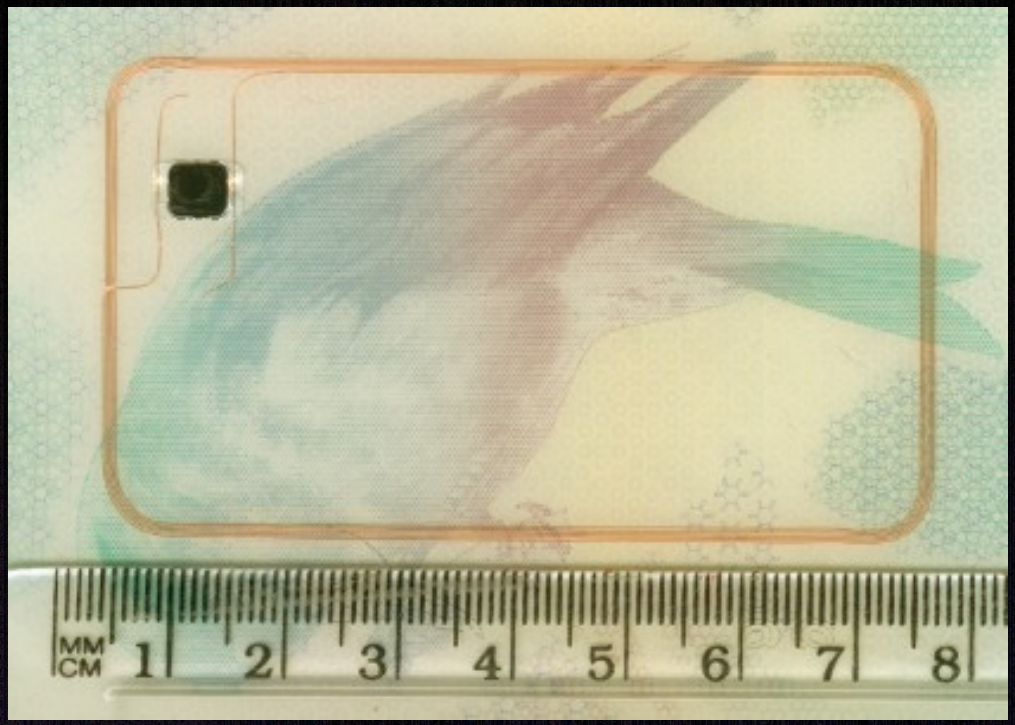


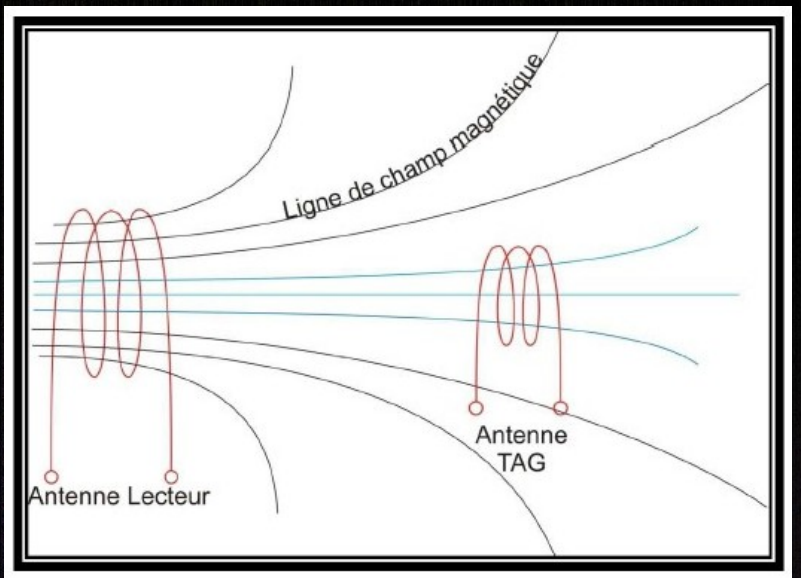


RFID (*Radio Frequency IDentification*)

Tag RFID = antenne + puce électronique

Tag passif, alimenté par lecteur pour interrogation et récupération des informations.



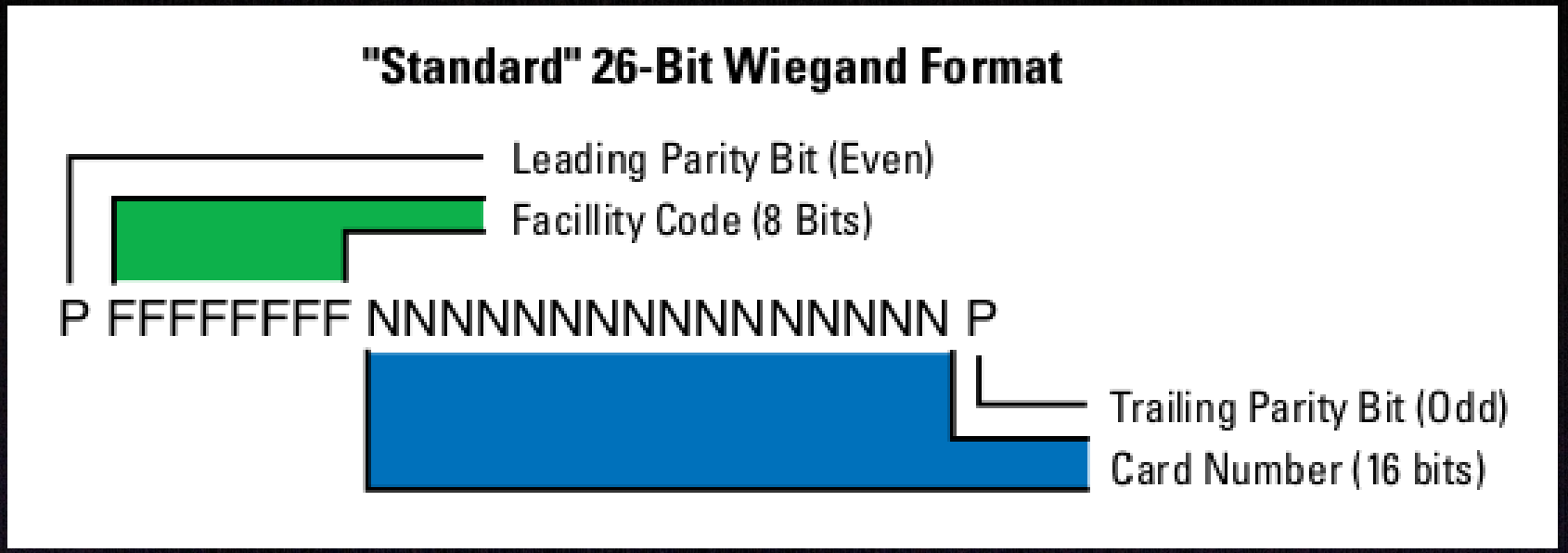


Couplage Magnétique
HF et LF
Champ proche

RFID – HID 'Prox'

Standard ouvert *HID 26 bits* ou *H10301*, toujours (très) utilisé pour le contrôle d'accès aux bâtiments.

125 Khz – Format Wiegand™ - 26 bits de data



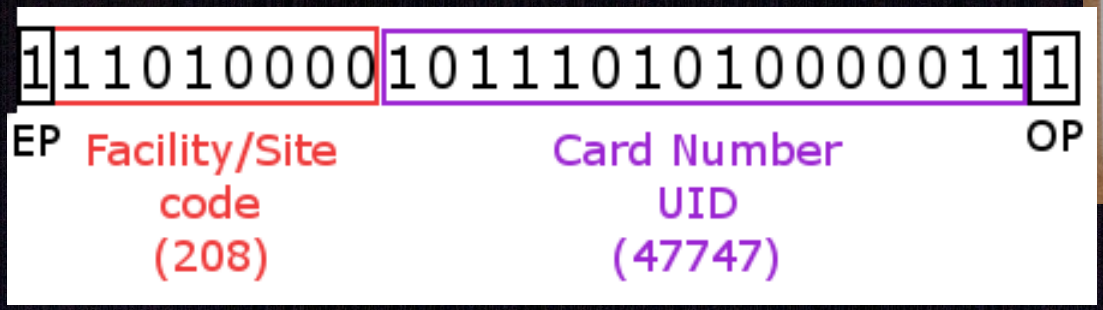
RFID – Lecture carte HID 'Prox'

Utilisation d'un Proxmark3:

.Mode LF (Low Frequency)

.Démodulation FSK (Frequency Shift-Keying)

```
D:\pm3-bin-20140401\win32>proxmark3.exe COM9
proxmark3> lf hid fskdemod
#db# TAG ID: 100ba17507 (47747)
#db# TAG ID: 100ba17507 (47747)
#db# TAG ID: 100ba17507 (47747)
```



AVRFID – le code

AVRFID utilise un ATtiny85 pour gérer:

.les données (type de carte + Site Code + UID)

.les protocoles d'échange (FSK)

```
/* tAd: using HID 26 bits only with PageMac website modifications (as HID_MFG_CODE) */
/* You can use http://www.brivo.com/support/card-calculator to calculate your SITE Code */

    #define HID_MFG_CODE        0x0801                  // do not modify
    #define HID_SITE_CODE       208
    #define HID_UNIQUE_ID       47747
```

```
* Basic schematic:
*
*                ATtiny85
*                +--------------+
*             --| RST      Vcc |--
*    +- L1 ----| B3/CLKI  SCK |--
*    +---------| B4       MISO|--
*             --| GND      MOSI|--
*                +--------------+
*
```

```
header

        manchester      HID_MFG_CODE, 19
        manchester      BIT_EVEN_PARITY, 1
        manchester      HID_SITE_CODE, 8
        manchester      HID_UNIQUE_ID, 16
        manchester      BIT_ODD_PARITY, 1

rjmp    loop
```

AVRFID – le code : compilation

Nécessite avr-gcc et avr-libc (sous Linux)

Livrés : 2avrfid(-tAd).S et Makefile

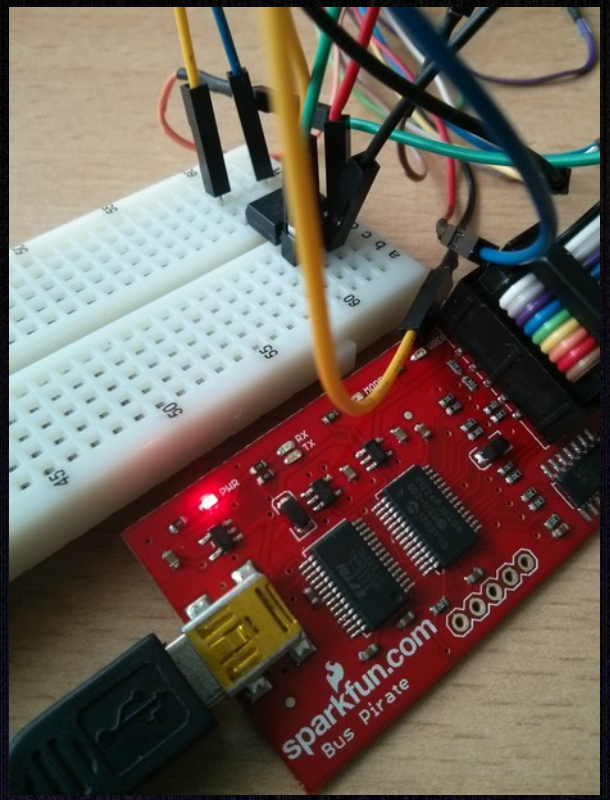
```
$ make
avr-gcc -mmcu=attiny85 -I. -gstabs -Os -Wall -Wstrict-prototypes -std=gnu99 -funsigned-char \
        -funsigned-bitfields -fpack-struct -fshort-enums 2avrfid-tAd.S --output avrfid.elf -lm
avr-objcopy -O ihex -R .eeprom avrfid.elf avrfid.hex
avr-objcopy -j .eeprom --set-section-flags=.eeprom="alloc,load" \
        --change-section-lma .eeprom=0 -O ihex avrfid.elf avrfid.eep
avr-objcopy: --change-section-lma .eeprom=0x0000000000000000 never used
```

AVRFID – le code : implémentation

.Utilisation de AVRDUDE avec un BusPirate

.Injection de *avrfid.hex* généré précedemment

```
$ avrdude -P /dev/ttyUSB0 -c buspirate -p t85 -v -U lfuse:w:0xC0:m -U flash:w:avrfid.hex
```



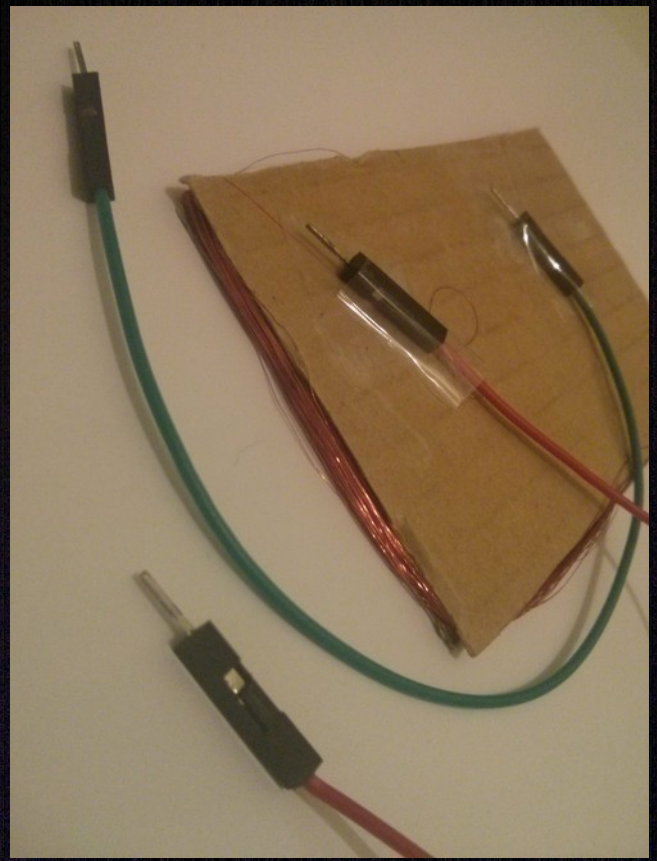
/!\ Nécessité de modifier les 'fuses' pour prendre en compte une fréquence d'horloge externe: l'antenne.

AVRFID – l'antenne

Une antenne DIY gérant le 125 KHz :

.un bout de carton ondulé (taille d'une carte)

.du fil de cuivre assez fin: une centaine de spires



Validation avec Proxmark:

Test entre pins TP2 et TP5,

Le mieux : entre 20V et 40V

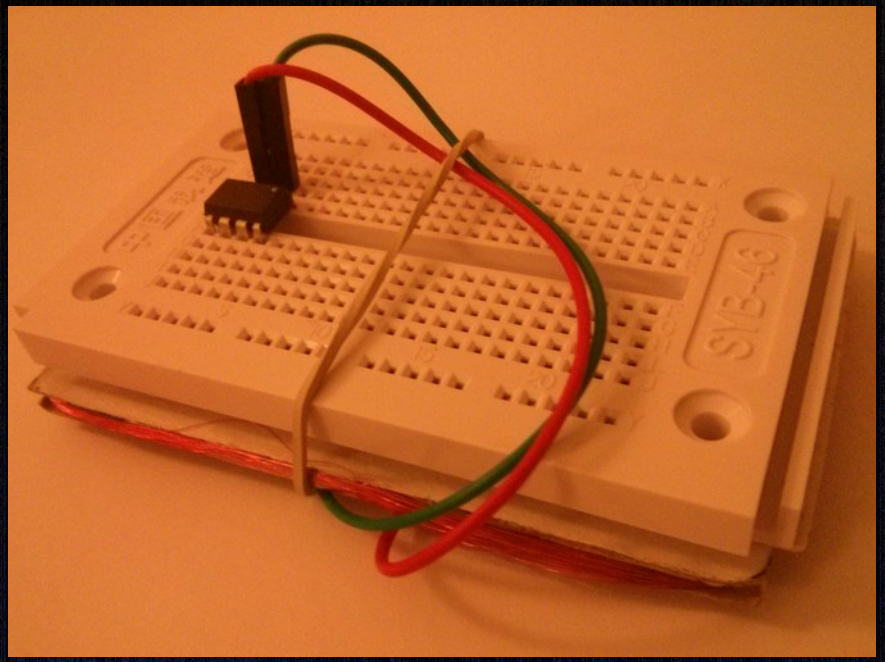
```
proxmark3> hw tune
#db# Measuring antenna characteristics, please wait...
#db# Measuring complete, sending report back to host

# LF antenna: 15,31 V @   125.00 kHz
# LF antenna:  9,27 V @   134.00 kHz
# LF optimal: 30,88 V @   115,38 kHz
# HF antenna:  0,16 V @    13.56 MHz
# Your HF antenna is unusable.
proxmark3>
```

AVRFID – finalisation

→ antenne validée

→ code implémenté

.on relie l'antenne aux PIN2 et PIN3 de l'ATtiny



Validation avec lecteur:

```
D:\pm3-bin-20140401\win32>proxmark3.exe COM9
proxmark3> lf hid fskdemod
#db# TAG ID: 100ba17507 (47747)
#db# TAG ID: 100ba17507 (47747)
#db# TAG ID: 100ba17507 (47747)
```

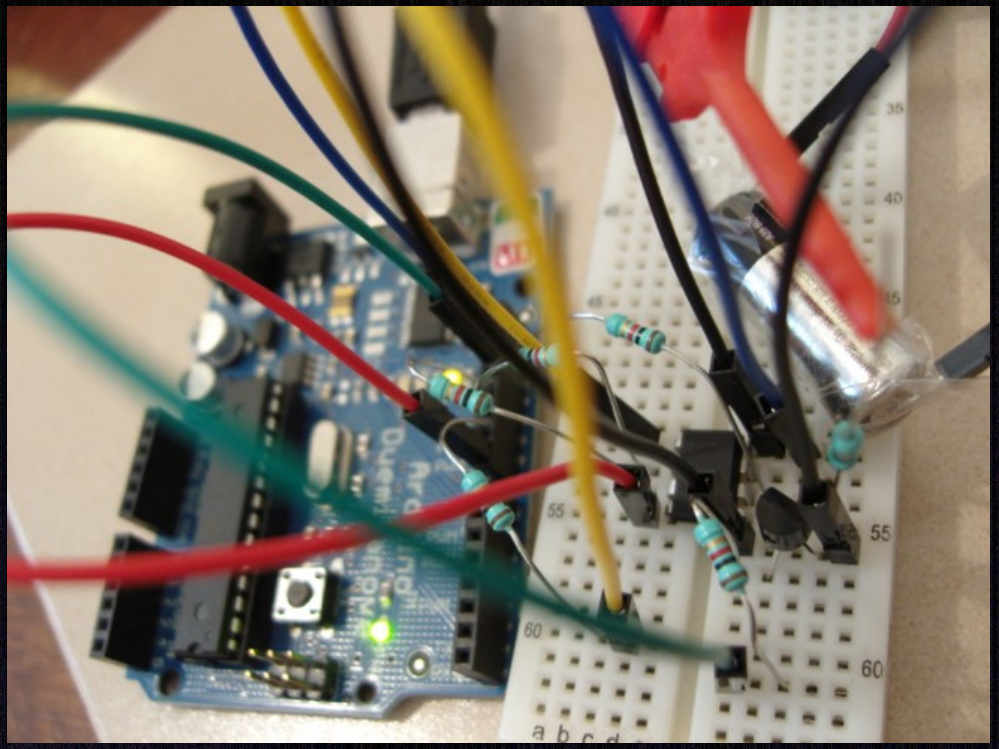
\o/

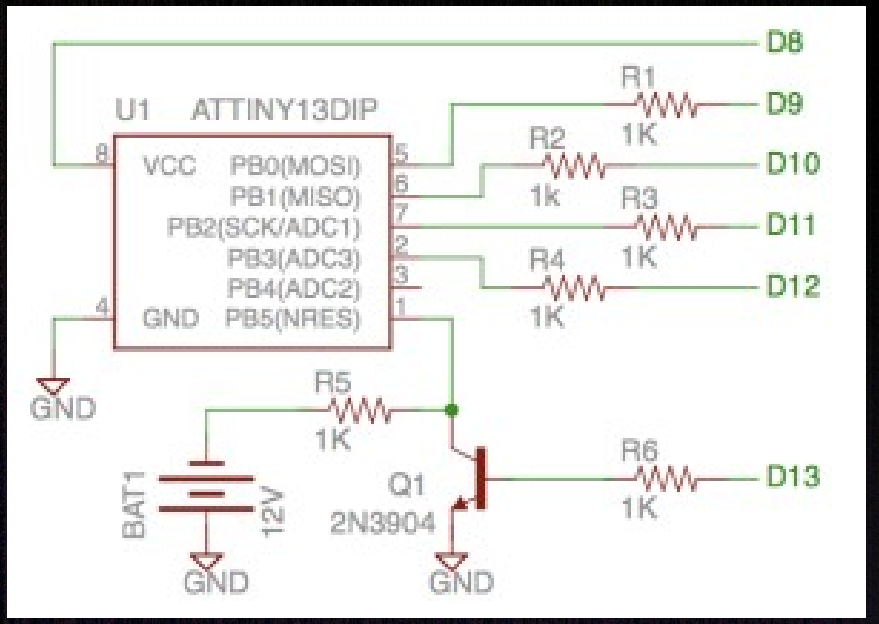
AVRFID – Modification

Rappel: les fuses ont été modifiés, push impossible

→ Nécessité de remettre les fuses à l'état initial.

Possible par application d'une forte tension:





https://o0tAd0o.wordpress.com

Recommandations

Faut plus utiliser cette techno!

Préférer des technos embarquant un minimum de crypto [ex: Mifare DESfire EV1 (Mutual authentication, AES 128, DES and triple-DES data encryption and unique 56-bit serial number.)] sur des lecteurs hybrides pour une migration en douceur…

Merci

AVRFID - tAd - BlackLoop